Mar 7th, 8:00 AM

System Reliability Mathmatical Modeling

Lee R. Webster
Electronics and Information Systems Division, Fairchild Hiller Corporation

SYSTEM RELIABILITY MATHEMATICAL MODELING

Lee R. Webster

ELECTRONICS AND INFORMATION SYSTEMS DIVISION

of

FAIRCHILD HILLER CORPORATION
Bladensburg, Md.

INTRODUCTION

The reliability mathematical model of a system is the basis of all reliability predictions, optimization, apportionment, and virtually all other system reliability analyses. Because of the importance of the math model, maximum care should be taken in its construction. A system reliability model is defined here as a probability expression which represents the actual system configuration such that when the reliabilities of the system elements are known along with certain other mission parameter values, the expression can be used to calculate the overall system mission reliability. The complexity of the model structure depends upon the complexity of the system it represents and upon the degree of accuracy used in approximating the actual system configuration. The well known series model, wherein the system reliability is given by the product of all the constituent element reliabilities is the simplest type. The accuracy of the series model will generally tend to be very high if the failure of any constituent element will cause the failure of the system of interest. However, more complex model types are required in order to accurately represent a system containing a relatively large number of alternate paths or modes of operation.

SUMMARY

This paper discusses the general procedures and considerations involved in the construction and improvement of system reliability models. Specific points covered include the performance of supporting operations analyses; the utilization of the system block diagrams and the failure mode and effect analysis in generating the system reliability diagram; and a summary of many of the more widely used mathematical tools used to transform the system function diagram into a system reliability expression.

The application of the procedure discussed is demonstrated on the Power Control and Conversion Assemblies of the Advanced Orbiting Solar Observatory (AOSO).

The AOSO Power Conversion and Control Assemblies are a portion of a project being performed for NASA by the Fairchild Hiller Electronics and Information Systems Division. These assemblies contain a large number of alternate operating modes and series-parallel situations which are used to satisfy an extremely high reliability requirement. These redundancy provisions plus a number of important but unknown quantities and other mission parameters, all of which must be taken into account, make the power control and conversion assemblies excellent examples for demonstrating the application of a wide variety of math modeling techinques.

MODEL CONSTRUCTION

Mathematical Tools

In a large majority of modeling situations, systems can be broken up into series or series-parallel combinations. The system reliability math model in these cases is constructed using one or more of a family of fairly widely known probability expressions and techniques. There are some configurations, however, which can not be expressed as combinations of series and/or parallel terms and therefore require more complex and somewhat less popular techniques. The following is a brief summary of the more widely used and fundamental procedures used in reliability math modeling.

Series

The simplest system model is the series configuration. In this model the system is represented as a chain and the total reliability is the product of all the individual element or link reliabilities. Thus, it is assumed that the failure of any element or link causes system failure and that system reliability is directly related to system complexity. For any given system and set of element failure rates, the value of system reliability which is predicted using a series model will be the minimum possible value and thus the most conservative. Because of the above, "parts count" reliability estimates are often used for making "ballpark" or "first cut" estimates of the reliability of a system.

Redundancy

When it becomes necessary to account for redundant system elements, various elements states, or alternate modes of system operation, the system math model becomes more complex. Before one can generate the reliability expression for redundant elements, it must be determined whether the back up elements are operating "on line" along with the main element or if they are on standby duty to be used only in the event of failure of the main element.

Functional Redundancy- When only one of a group of elements simultaneously operating in parallel is needed, the total reliability for the group is one minus the product of the element unreliabilities.*

*Note: This result neglects possible increases in element failure rates caused by increased loading resulting from the failure of other elements. This is one result of the assumption of statistical independence made for all elements throughout this paper unless otherwise specified.

$$R = 1 - \prod_{i=1}^{n} q_i$$

Where:

R = total reliability of the group of redundant elements.

q_i = the unreliability of the i th element

n = number of elements in parallel

Similarly, if all the elements have equal reliabilities, the group reliability R, then becomes:

$$R = 1 - q_i^n$$

This last result is also obtained from expansion of

$$(r+q)^n = 1 = r^n + nr^{n-1}q + \cdots + q^n$$

where

r = the reliability of each of the i elements

n = the total number of parallel elements

As before q^n is the probability of all n units failing and $1-q^n$ is the probability of at least one unit operating, i.e. the group reliability.

Many times it becomes necessary to account for differences in element failure modes. For example, if an element can fail only as an open circuit and if n are arranged as in Figure 1, the group reliability is found from the previously given expression

$$R = 1 - q^n$$

If, however, the above elements are arranged in series, the group reliability becomes r^n since the opening of any one element causes the whole group to fail. Similarly then, it can be seen that if elements which fail only as short circuits are arranged per figure 1, the group reliability becomes r^n since the shorting of any one element results in total group failure. Thus, it follows by placing elements which fail only by shorting in series the group reliability is given by:

$$R = 1 - q^n$$

Sequential Redundancy - When only one of a group identical elements is in use while the remainder are in a non-operating stand-by status waiting to be switched in one by one upon failure of the operating element, the total reliability is given by
(neglecting switching reliability)

$$R = e^{-\lambda t}\left[1 + \lambda t + \frac{\lambda^2 t^2}{2!} + \cdots + \frac{\lambda^n t^n}{n!}\right]$$

Where:

e = base of the natural log system

λ = the failure rate of each of the n elements

t = mission time

If the operating and the non-operating standby elements have different reliabilities, the total reliability for the group requires the integration of the joint density function of the combination. This is a very general procedure being applicable regardless if the elements are equal or if they have exponential reliability functions. In cases where the element reliability functions are exponential, the density function $f(t)$ is given as:

$$f(t) = \lambda e^{-\lambda t}$$

For two different elements having failure rates λ_1 and λ_2, the density functions are respectively,

$$f_1(t) = \lambda_1 e^{-\lambda_1 t}$$

$$f_2(t) = \lambda_2 e^{-\lambda_2 t}$$

where:

t_1 = time of failure of element number 1

$t - t_1$ = time of failure of element number 2 = t_2

t = mission time

The probability of both elements failing in an infinitely small time interval t, $t + dt$ is the product of the two density functions. Integrating this product from $t_1 = 0$ to t_1 = mission time, t, obtains the joint density function, $F(t)$ for the two element combination in terms of the single variable t.

$$F(t) = \int_{t_1=0}^{t} f_1(t_1) f_2(t - t_1)\, dt_1$$

again looking at the exponential use this result is

$$F(t) = \lambda_1\lambda_2\left(\frac{e^{-\lambda_1 t}}{\lambda_2 - \lambda_1} + \frac{e^{-\lambda_2 t}}{\lambda_1 - \lambda_2}\right)$$

The integration of this result, with respect to time from t to infinity is the summation of all possible combinations of the time of failure for elements 1 and 2 which result in the system failing after mission time t and is therefore the combined reliability R, for the two element arrangement (again neglecting switching reliability).

$$R = \int_t^{\infty} F(t)\, dt$$

and for the exponential case

$$R = e^{-\lambda_1 t} + \frac{\lambda_1}{\lambda_2 - \lambda_1}\left(e^{-\lambda_1 t} - e^{-\lambda_2 t}\right)$$

Functional and Sequential Redundancy Combinations

Other types of redundancy which are variations of the sequential and/or functional type are given in Table I. Also included in the table are reference sources which provide more complete information on the derivation of the probability models listed.

Bayes' Theorem- Occasionally a system configuration will be encountered in which the elements are not arranged in series or combinations of functional or sequential redundancy.

One example of such a case would be a configuration such as shown in Figure 2. In this system, the successful or operating states which are possible are AB, CB, CD, and ED. Thus, unlike the redundancy configuration on Figure 3, the combinations AD and EB are not possible. Bayes' Theorem states that if I is an event which depends upon one of two mutually exclusive events, H and J, of which one must necessarily occur, then the probability of the occurence of I is given by

$$P(I) = P(I \text{ given } H) \cdot P(H) + P(I \text{ given } J) \cdot P(J)$$

Applying Bayes' Theorem to block C of the system in Figure 2, the following can be stated:

$$P(\text{SYSTEM FAILURE}) = P(\text{SYSTEM FAILURE IF C IS GOOD}) \cdot P(\text{C IS GOOD}) + P(\text{SYSTEM FAILURE IF C IS BAD}) \cdot P(\text{C IS BAD})$$

$$= (1-R_B)(1-R_D)R_C + (1-R_A R_B)(1-R_E R_D)(1-R_C)$$

System Reliability Diagram

Simply stated, the reliability diagram is a schematic representation of the system functions and subfunctions combined in a probability sense rather than signal flow. The system reliability diagram serves as a basis for making the transistion from the system functional block diagram to the system reliability math model. This is because the math model is merely mathematical expression for the logic implicit in the reliability diagram. A typical reliability diagram is generated in the following example: Figure 4 is a signal flow or functional block diagram of an engine starting circuit for an automobile. Figure 5 is the reliability diagram of the same system. Although a number of elements in Figure 4 are wired in parallel, in a reliability sense all these elements are in series since they are all needed to start the engine.

The simplicity of the reliability diagrams in the above example is the exception rather than the rule.

Nearly all reliability diagrams (and math models) are approximations. As such, the two essential characteristics of the system reliability diagram are that it be sufficiently representative of the system operation and that it not be so complicated as to make the resulting math model unusable. The satisfaction of both of the requirements becomes increasingly difficult as the system complexity increases and requires considerable interplay of the system design engineering, operations analysis, and reliability engineering disciplines. In many instances, for example, it is a considerable task to define such a basic concept as system or mission success.

The system reliability block diagram should be constructed as early as possible in the evolution of the system configuration. This will permit the analyst to give full consideration to design audit and failure mode and effect analysis data in up dating the construction of the math model. By virtue of the increased accuracy of the math model and its availability early in the project, the reliability engineer is in a position to not only more realistically monitor the quality of the design job but also to provide design engineering with better analytical support for design improvement and optimization which will be discussed later.

Returning to the engine starting problem, Figure 6 shows an improved reliability block diagram which includes failure mode and effect analysis data. In this diagram it can be seen that the manual crank is effective only if the starter and/or solenoid has failed open, and if the battery has been discharged less than 70%. This shows that the probability of at least turning the engine over either electrically or manually during the starting process is less than unity which is implied in Figure 5.

System Reliability Math Model

After the reliability block diagram has been generated, the system reliability math model is constructed by utilizing a variety of mathematical tools and probability expressions, such as surveyed earlier, to develop and combine expressions for subassembly and/or subfunction reliabilities. When these subassembly and/or subfunction reliabilities are quantized, the model can be solved to predict system reliability.

MODEL USE

Although the system reliability math model is probably most widely used for performing reliability predictions, there are a number of other important applications which can be made in an efficient, modern reliability program. These additional applications include design reliability optimization, system effectiveness analysis, and technical management decision making.

Design Reliability Optimization

The function of optimizing the reliability of a design is defined here to be the selection of that system configuration, from the family of all possible configurations which are acceptable for a given task, which has optimum values of reliability and other system parameters such as weight, cost, etc. In general, there are two types of reliability optimization problems.

Problem Type I. In what is called here a type I problem, a system reliability requirement is specified and it is desired to obtain a system configuration which just satisfies this requirement and which also satisfies other constraints which may be stated or implied. An example would be to configure a system such that it has a 90% reliability, a maximum weight of 100 lbs., and a minimum cost.

Problem Type II. The second type problem is essentially the reverse of Type I. The objective in this problem is to configure a system which has the maximum reliability possible while still satisfying all other specified constraints. Such as maximum levels of weight, volume, and cost.

There are a number of optimization procedures available and undoubtedly many improvements are forthcoming as a result of the increasing research activity in this area. The use of one of these methods will be briefly demonstrated herein on a portion of a satellite power system.

System Effectiveness Analysis

By including system deployment variables such as maintainability, down times, etc., into the construction of the reliability math model, a figure of merit for system effectiveness is obtained.

Performing design reliability optimization analyses with the inclusion of deployment variables information then implies the derivation of a system configuration having an optimum or maximum effectiveness.

Technical Management Decision Making

If the reliability math modeling process is begun early and kept current throughout the R & D effort, it is a relatively simple task to utilize the model to obtain information very useful in directing engineering effort, design emphasis, and system philosophy. Relatively minor analyses can be performed during preliminary design in order to competitively evaluate alternate system philosophies, identify reliability limitations posed by state of the art requirements, and having selected a system philosophy, to design both a reliability and a development program plan. During the progress of the development effort, the same type of analysis as performed above will assist in isolating and assessing requirements for shifts in engineering effort and/or emphasis.

Reliability Model for AOSO Power Control and Conversion Assemblies

Problem

The reliability mathematical model construction and use techniques are demonstrated in the following discussion of the AOSO (Advanced Orbiting Solar Observatory) power control and power conversion assemblies. The specified mission for AOSO is a 70% reliability for one year of orbital operation. The apportioned reliability requirements for the power conversion and control assemblies for the one year mission are 94.3% and 97.1% respectively. There is an additional requirement of a 0.915 reliability for the combination of both assemblies.

Model Construction

First Estimate- The "first cut" or "ball park" reliability estimate of the subject assemblies was based strictly upon a parts count prediction. Although the resulting predicted reliability value of 0.513 was comparatively low, it was also obvious that the use of the series model or parts count approach was too conservative and that a number of mission parameters needed to be quantized.

Operations and System Analysis- In order to better define the existing system configuration and the mission requirements for the two assemblies, extensive operations and system analyses were undertaken.

System Analysis- In analyzing the system, reliability and design engineers concentrated primarily on the completion of a preliminary failure mode and effect analysis (FMEA). This analysis established the cause, type, and probability of occurence of subassembly failure and determined the consequences of these failures to the operation of the two assemblies with respect to degradation of output and to the availability of alternate modes of operation. In addition, the system was also broken up into specific functions which were defined, classified, and related to appropriate circuitry and/or subsystems.

The results of the system analysis included such items as the following:

1. The functions of taper (high rate Charging) and trickle (low rate charging) of the satellite batteries by the control assembly were identified and the conditions under which each can be performed were determined.

2. The actual redundancy in the solar paddle deployment squid firing circuits of the control assembly was determined.

3. Since the non-operating standby battery has a predictable loss of charge rate under open circuit conditions at the design ambient temperature, the trickle charging of the standby battery need only be supplied for the first 7792 hours of the mission.

Operations Analysis. This effort consisted of the AOSO mission requirements to determine the more specific mission requirements for the power conversion and control assemblies. In addition, there was a joint effort with the AOSO prime contractor to perform a failure mode of operation study. This study was an overall AOSO system investigation into what type of assembly failures actually caused mission abort. (This is a different goal than for the failure mode and effect analysis performed during the system analysis which considered performance outside of assembly specification limits as a failure).

The results of these studies included the following:

1. Reliability calculations should be based on a mission time of 8800 hours instead of 8760 in order to account for the increased environmental severity during launch.

2. Although only one battery is needed for operation, thus leaving the remaining battery as a non-operating standby unit, the mission of the conversion and control assembly must be able to maintain either battery at full charge for one year. Thus, the redundancy advantage is taken into account in the overall AOSO system analysis.

3. Due to the more or less linear decay (caused by radiation) of the power generating capabilities of the solar paddles with respect to time, the solar array voltage limiter is actually needed only for approximately the first 4000 hours of the one year flight.

System Reliability Diagram The results of the operations and system analyses described above were used in the first attempt to construct the reliability block diagram of the conversion and control assemblies (Figures 7, 8, 9.)

Figure 7 merely shows the series relationship between the control and conversion assemblies, i.e. both are needed for mission success.

Figures 8 and 9 are reliability diagrams of the power control assembly and the battery charge regulation function of the control assembly, respectively. No figure is included for the power conversion assembly since, during this phase of the AOSO Program, it was simply a series string of assemblies as will be described later.

System Reliability Math Model In developing the mathematical models for the power conversion and control assemblies, the following assumptions and conditions are made:

1. The power control assembly requirement is interpreted as follows:

   The power control assembly shall have a 97.1% probability of maintaining a full charge on a specified Operating Battery and a Standby Battery for a mission duration of 8800 hours. (note that this provision neglects the fact that the batteries are redundant by essentially stating that both are needed.)

2. The failure of a State of Charge Monitor is assumed to result in an open, such that the associated battery must be utilized in the circuit through an alternate route.

   If the original Operating Battery loses 80% of its charge as indicated by its state of charge monitor, or has a State of Charge Monitor failure, it is replaced by the Standby Battery. Emergency mode operation is initiated whenever both batteries are below 50% of charge. It is assumed that the emergency mode merely provides the system, upon ground command switching, with the capability that either charger can be used to charge either of the two batteries on the line (See Figure 9) Time consumed in having to recharge dead batteries and problems in removing (if required) catastrophically failed units from the line are not considered.

3. The definitions of taper and trickle charge used herein are somewhat broader than the usual technical definitions. Essentially, taper charging is used to designate a high charge rate as opposed to trickle charging which is that charge rate used to maintain a full charge on the Standby Battery. Thus, the battery charge regulation function is said to contain one Taper Charger, one Trickle Charger, and a Backup Charger which has a taper charge mode and a trickle charge mode.

4. The taper charge mode of the Backup Charger is assumed to be useable only when the Taper Charger has failed or when the power control assembly is in the emergency mode of operation.

5. The trickle charge mode of the Backup Charger is used to replace the failed Trickle Charger only if the Taper Charger has not failed. In addition, it is assumed that both the Trickle and Taper Charging modes of the backup charger have the same failure rate.

6. The Backup Charger is assumed to have a non-operating standby failure rate equal to zero.

7. Ambient battery temperatures are assumed to be equal to the maximum design temperature of 110 F for purposes of deriving the period of time required by a fully charged battery to lose 50% of its charge, while on non-operating standby and open circuit conditions.

8. Ambient power control and power conversion assembly temperatures are assumed to be 150°F.

9. All elements are assumed to have an exponential reliability distribution.

10. Only "on board" electronics and/or systems are considered. Ground based equipments, signal conditioning circuits, and human inputs are neglected.

11. The reliability of the switching functions shown as items (4), (5), (6), (7), (9), and (12) in Figure 9 is assumed to be independent of time and refers to a single switchover operation.

12. The life of a State of Charge Monitor is small compared to the life of a battery.

13. Modes of degraded system operation, such as those employing the trickle charger when the taper and backup chargers have failed, are not considered.

14. The advantages of making more than one change between primary and backup charge modes are not considered.

15. At least one source of trickle charge is required for the standby battery from start of mission to 7792 hours.

16. No provision is made for epoxy covered solder connections.

Power Control Assembly - Figure 8 is the reliability diagram for the four functions performed by the power control assembly. As shown in Figure 8 the Power Control Assembly will satisfy its mission requirements if:

1) The hold-off function is performed properly prior to and at the initiation of launch.

2) The paddle deployment function is satisfactorily completed when initiated.

3) The battery charge regulation function is performed for one year, and

4) The solar array voltage limiter function is satisfactorily performed for one year.

Referring to Figure 8, the expression for the reliability, R(PCA), of the Power Control Assembly is:

$$R(PCA) = R(HO)\ R(PD)\ R(BCR)\ R(SAVL)$$

where:

R(HO) = the reliability of the Hold-Off Circuitry

R(PD) = the reliability of the Paddle Deployment circuitry

R(BCR) = the reliability of the Battery Charge Regulation function

R(SAVL)= the reliability of the Solar Array Voltage limiter function

The Hold-Off and Paddle Deployment functions are performed by series type electronic circuitry. The reliability of the devices providing these functions is represented by the product of the reliabilities of the piece parts that compose the devices. Therefore:

$$R(HO) = \prod_{i=1}^{n_1} R_i$$

and

$$R(PD) = \prod_{j=1}^{n_2} R_j$$

where: R_i = the numerical reliability of the ith piece part in the Hold-Off circuitry

n_1 = the total number of piece parts that make up the Hold-Off circuitry

R_j = the numerical reliability of the jth piece part in the Paddle Deployment circuitry

n_2 = the total number of piece parts in the Paddle Deployment circuitry

Figure 9 is the reliability diagram for the Battery Charge Regulation function. The Battery Charge Regulation function is provided by a Taper Charger, a Trickle Charger, a Backup Charger with both a taper and trickle charge capability, two State of Charge Monitors each associated with a particular spacecraft battery, and a group of logic and switching circuits. The Battery Charge Regulation function is satisfactorily performed if the Operating Battery (either Battery A or Battery B) receives a taper charge and the Standby Battery (Battery B or Battery A) receives a trickle charge.

In the primary mode of operation the Taper Charger feeds the Operating Battery through its associated State of Charge Monitor and the Trickle Charger feeds the Standby Battery directly. Under these conditions, the Backup Charger is maintained in a non-operating standby status.

If the Operating Battery State of Charge Monitor fails, the Taper Charger can be switched through the Ground Command Bypass Loop to the Operating Battery. If the Taper Charger fails, or it both the State of Charge Monitor and the Cround Command Bypass Loop fail;

1) a ground command can turn on the taper charge mode of the Backup Charger and feed the Operating Battery from the Backup Charger

2) The operating and Standby Batteries are interchanged automatically by the battery selector switch or by the Ground Command Modules Nos. 7 and 9. This operation also requires successful operation of the Ground Command Module No. 6 which switches the Taper Charging Function to the new operating battery.

3) if both batteries are below the prescribed level of charge, the emergency mode is initiated, or

4) both the Operating and Standby Batteries are brought on the line by the action of two zener diodes when the line voltage drops more than 12 volts below the highest terminal voltage of the two batteries

In the event of (3) or (4) above, taper charging is supplied both batteries simultaneously by the taper charger or the backup charger.

If the Trickle Charger fails, a ground command must turn on the trickle charge mode of the Backup Charger (assuming the Backup Charger is not then feeding the Operating Battery) and feed the Standby Battery from the Backup Charger.

Referring to Figure 9 , the Battery Charge Regulation function will be satisfactorily performed if the Common Selector Logic does not fail, and if either:

1) The Taper Charger (1) charges the Operating Battery either through the associated State of Charge Monitor (2), or through the Ground Command Number One Bypass loop (12), or

2) If the Ground Command Switch (4) turns on the taper charge mode of the Backup Charger (3) which then charges the Operating Battery

In addition, success has been assumed to imply that a charge is maintained on the Standby Battery (see assumption 1). Therefore, successful performance of the Battery Charge Regulation function also requires that:

1) The Trickle Charger (8) operates satisfactorily, or that

2) The Ground Command Switch (5), the taper charger (1), and the trickle charge mode of the Backup Charger (14) operate satisfactorily (see assumption 5), or that

3) The Emergency Mode functions properly or that

4) The Battery Selection Mode does not fail

Proper operation of the Standby Battery implies that it be charged to at least 50 percent of its capacity at the time it is switched to Operating Battery status.

Presently available information indicates that a fully charged nickel-cadmium battery at the maximum AOSO temperature of 110°F, under no-charge, no load conditions, will lose 50 percent of its charge in 42 days (1008 hours). Therefore, the Standby Battery must receive a trickle charge from the state of the mission, until no more than 42 days before failure of the Operating battery. If the primary trickle charge mode (that is, if the Trickle Charger itself) fails, the trickle charge mode of the Backup Charger will be switched on and will feed the Standby Battery. This assumes that it is not already supplying the Operating Battery (see assumption 5). The trickle charge mode of the Backup Charger will then be required to operate without failure from the time of the failure of the Trickle Charger until no more than 42 days before failure of the Operating Battery.

Lack of information prevents the identification of the reliability distributions of the AOSO batteries at this time. Even if this information were available, the derivation of a precise expression for the probability of successful performance of the trickle charger function would require the summation of all successful combinations of Taper Charger, Trickle Charger, and Backup Charger success and failure, along with conditional probabilities associated with the performance of the Operating Battery over the time interval from $\tau = 0$ to $\tau = t$ (end of mission). The result is a very unwieldy set of integrals. In order to elevate this situation, it is specified (see assumption 16) that either the Trickle Charger or the trickle charge mode of the Backup Charger must operate from the start of the mission to within 42 days or 1008 hours before the end of the one year mission time, t. The resulting expression is conservative in that it completely neglects all those combinations of circumstances in which successful system operation will result in spite of failure of both the Trickle Charger and the trickle charge mode of the Backup charger prior to t - 1008 hours or 7792 hours.

The Common Selector Logic shown in Figure 9 consists of two silicon controlled rectifiers (SCR). The reliability R(CSL), of the Common Selector Logic is merely the product of the reliabilities for the SCR's.

$$R(CSL) = \prod_{i=1}^{2} R(SCR)_i$$

The reliability for the Emergency Mode is essentially determined by the emergency mode circuitry. There is, however, a backup for this circuitry. The backup for the emergency mode circuitry consists of two zener diodes which cause both batteries to be switched on to the main line whenever the line voltage drops more than 12 volts below the highest of the two battery terminal voltages. Because of the different operating principles employed, this backup system does not act to remove non-essential loads from the line and will require a larger time delay for operation. Therefore, the backup system is not operationally equivalent to the emergency mode circuitry, although these alternates are considered equal in the development of the mathematical model. The reliability, R(EM), of the Emergency Mode is then the probability that either the emergency mode circuitry (R_{10}) or its backup circuitry (R_{11}) operates.

$$R(EM) = 1 - (1 - R_{10})(1 - R_{11})$$

The reliability of the battery selection mode R(BS) is the probability that the Ground Command Module No. 6 operates times the probability that either the battery selection circuitry or the Backup Ground Command Modules Nos. 7 and 9 operate. The reliability of the selection circuitry is equal to the probability, R_6, that both battery sensors operate times the probability, R_a, that both sensor modules operate, times the probability, R_{CD}, that the C, C_1, and D logic modules operate. Thus,

$$R(BS) = R_6\,[1 - (1 - R_a R_a R_{CD})(1 - R_7 R_9)]$$

The reliability, R(BCR), of the Battery Charge Regulation function can now be expressed as a function of the respective reliabilities of the Common Selector Logic, R(CSL), and of the devices involved in the primary, backup, and emergency modes of operation.

Let:

- F = the probability of failure of the primary charge mode in the time period Δt_i
- $R(BCR)$ = the reliability of the Battery Charge Regulation function
- t = the total mission time of 8800 hours
- R_i = the reliability of the ith device in the Battery Charge Regulation function and i = 1, 2, 3, . . . corresponding to the numbering of the blocks in Figure 9.
- f_2 = the probability of failure of the Operating Battery State of Charge Monitor in the time period
- $R_3(t-t_1)$ = the probability of successful operation of the Backup Charger from the time of failure of the primary charge mode, t_1, to the end of the mission, t
- G = the probability of failure of the Trickle Charger in the time period
- $R_9(t-1008-t_2)$ = the probability of successful operation of the trickle charge mode of the Backup Charger from the time of failure of the Trickle Charger, t_2, to t - 1008 hours
- $R(EM)$ = emergency mode reliability
- $R(BS)$ = battery selection mode reliability
- $R(CSL)$ = Common Selector Logic reliability

(Note assumption 12 regarding the time independence of the switching devices (4), (5), (6), (7), (9), (12))

Then: R(BCR) =

$$\left[R_1(R_2 + R_{12}\int_0^t f_2 d\tau) + R_4\int_0^t FR_3(t-\tau_1)d\tau_1\right]\left\{1 - \left[1-\left(R_8 + R_1 R_5 \int_0^{t-1008} GR_{14}\,(t-1008-\tau_2)d\tau_2\right)\right]\left[1-R(EM)\right]\left[1-R(BS)\right]\right\} R(CSL)$$

The Solar Array Voltage Limiter function is provided by a difference amplifier, a driver stage, and a power stage. Satisfactory performance of the Solar Array Voltage Limiter function requires that all three devices perform satisfactorily. Therefore, the general expression for the reliability of the Solar Array Voltage Limiter function, R(SAVL), is:

R(SAVL) = R(DA) R(DS) R(PS)

where:

R(DA) = the reliability of the Difference Amplifier

R(DS) = the reliability of the Driver Stage

R(PS) = the reliability of the Power Stage

Both the Difference Amplifier and the Driver Stage are series type electronic circuits. The reliability model for each device is, therefore, simply the product of the reliabilities of the piece parts that make up the device. If:

R_k = the reliability of the kth piece part in the Difference Amplifier, and

n_3 = the total number of piece parts in the Difference Amplifier, the reliability model of the Difference Amplifier is given by:

$$R(DA) = \prod_{k=1}^{n_3} R_k$$

Similarly, if:

R_m = the reliability of the mth piece part in the Driver Stage, and

n_4 = the total number of piece parts in the Driver Stage, the model of the reliability, R(DS), of the Driver Stage is given by:

$$R(DS) = \prod_{m=1}^{n_4} R_m$$

The power stage consists of nine parallel branches, each comprising a transistor and a resitor. Proper operation of the Power Stage requires that the first two branches be fed by the Driver Stage, and any four of the remaining seven branches operate satisfactorily. Each branch is fused. Therefore, only "open" type failures are possible. To derive the mathematical model of the reliability, R(PS) of the Power Stage, let:

r = the reliability of any one of the nine parallel branches, and

q = the unreliability of any one of the branches

Then the mathematical model is given by:

$$R(PS) = r^2(r^7 + 7r^6q + 21r\,q^2 + 35r\,q^3).$$

Substituting the derived mathematical models in the general expression yields the mathematical model for the reliability of the Solar Array Voltage Limiter:

$$R(SAVL) = \prod_{k=1}^{n_3} R_k \left[\prod_{m=1}^{n_4} R_m\right]\left[r^2(r^7 + 7r^6q + 21r\,q^2 + 35r^4q^3)\right]$$

Summary:

In summary, the general expression for the reliability of the power control assembly in terms of the reliability of the functions performed by the power control assembly equipment, is:

R(PCA) = R(HO) R(PD) R(BCR) R(SAVL)

Since:

R(HO) = the reliability of the Hold-off circuitry

$$= \prod_{i=1}^{n_1} R_i,$$

R(PD) = the reliability of the Paddle Deployment circuitry

$$= \prod_{j=1}^{n_2} R_j,$$

R(BCR) = the reliability of the Battery Charge Regulation function

$$= \left[R_1(R_2 + R_{12}\int_0^t f_2\,d\tau_1) + R_4\int_0^t FR_3(t-\tau_1)d\tau_1\right]\left\{1-\left[1-(R_8 + R_1'R_5\int_0^{t-1008} GR_{14}\,(t-1008-\tau_2)\,d\tau_2)\right]\left[1-R(EM)\right]\left[1-R(BS)\right]\right\} R(CSL)$$

R(SAVL) = the reliability of the Solar Array Voltage Limiter

$$= \left[\prod_{k=1}^{n_3} R_k\right]\left[\prod_{m=1}^{n_4} R_m\right]\left[\lambda^2(\lambda^2+7\lambda^6 g+21\lambda^5 g^2+35\lambda^4 g^3)\right]$$

the reliability mathematical model of the power control assembly is:

$$R(PCA) = \left[\prod_{i=1}^{n_1} R_i\right]\left[\prod_{j=1}^{n_2} R_j\right]\left[R_1(R_2+R_{12}\int_0^t f_2\,dT) + R_4\int_0^t FR_3(t-T_1)\,dT_1\right]\cdot \left\{1-\left[1-R_7+R_7R_1'\int_0^{t-1008} GR_{14}(t-1008-T_2)\,dT_2\right]\left[1-R(EM)\right]\cdot \left[1-R(BS)\right]\right\} R(CSL)\left[\prod_{k=1}^{n_3} R_k\right]\left[\prod_{m=1}^{n_4} R_m\right]\left[\lambda^2(\lambda^2+7\lambda^6 g + 21\lambda^5 g^2+35\lambda^4 g^3)\right]$$

The predicted reliability resulting from the solution of the above model is the probability that a taper charge and a trickle charge will be available for an Operating Battery and a Standby Battery, respectively, for a period of 8800 hours in orbit. This is a very conservative statement of the mission problem, however, since all that is required for AOSO success is the ability to taper charge either of the two batteries.

The model describing this latter problem would not require that the Trickle Charge Function not fail. Instead, a conditional probability would be associated with the requirement for the Trickle Charge Function for mission success. Thus, (referring to Figure 9) the taper charge function would be directly connected to the Operating Battery and the Trickle Charge Function, the Emergency Mode, or the Battery Selection Mode would be utilized only with the condition that the Operating Battery fails. A reliability value cannot be calculated from this latter model at present, however, since nothing is known about the probability of having to switch from the Operating to the Standby Battery and, as mentioned earlier, the accounting for the redundant batteries will take place in the over all AOSO analysis performed by the prime contractor.

Power Conversion Assembly - The mathematical model of the reliability of the Power Conversion Assembly is relatively simple. There are 14 subassemblies that make up the Power Conversion Assembly. All of these subassemblies must operate properly if the Power Conversion Assembly is to satisfy its requirements. Therefore, the reliability of the Power Conversion Assembly is simply the product of the reliabilities of the 14 subassemblies. Mathematically, this is expressed as

$$R(\text{Power Conversion}) = \prod_{i=1}^{14} R_i$$

where:

R = the reliability of the ith subassembly

Model Use

System Reliability Prediction - The quantative analysis consists of the evaluation of the mathematical models derived above. In order to perform this evaluation, a tabulation of part types, quantities, and failure rates are made for each of the blocks in the reliability diagram. This tabulated information permits the calculation of the subassembly reliabilities which are then combined in the manner prescribed by the reliability mathematical models. The results of reliability predictions using the math model developed above are shown in Table II.

Reliability Optimization - The results of above prediction indicated that the reliability of the conversion assembly needed to be improved from 0.797 to 0.943. There was also a strong indication that changes were needed in system design philosophy.

First of all, it was readily apparent that preliminary designers were somewhat overly concerned with being able to perform and control the battery charge and discharge functions. This resulted a large number of separate alternate modes of operation which, from the weight viewpoint caused the assembly to be too reliable. This meant that the control assembly could be simplified at a saving in weight and volume which would be invested into increasing the reliability of conversion assembly.

Another preliminary design concept requiring review was the effort to stay away from power supply switching problems and very costly weight and volume penalties which would be associated with the employment of redunancy in the conversion assembly. The use of ultrareliable Minuteman Project parts to negate the need for redundancy was one of the main results of this concept. The reliability prediction, however, revealed that the use of minuteman parts resulted in the conversion assembly reliability being almost entirely a function of the reliability of electrical connections. Further, it was apparent that the failure rate of soldered or welded connections would have to be decreased by two orders of magnitude before the initial conversion assembly configuration could meet the reliability requirements.

In order to determine what new concepts should be adopted for the purpose of generating a design configuration with acceptable reliability, the system math model was subjected to an optimization effort throughout the design period. The initial procedures and results of this effort are covered in reference 2.

The mathematical development and supporting theory for the optimization procedures used on power control and conversion assemblies are contained in references 10, 12 and 13. In brief, these procedures permit simultaneous consideration of n methods of subassembly reliability improvement, such as different types of redundancy, and m system parameters, such as weight and volume, in order to select the optimum system configuration.

The governing analytical process consists of the identification of the area of least reliability in the system and the selection of the technique for increasing the reliability of that area which is best with respect to system parameters such as weight and cost. This process is repeated with each new "least reliability area" until an optimum system is achieved. The optimum

system is that final system configuration in which the reliability of the least reliable area has been maximized to a degree which assures satisfaction of the system reliability requirement without exceeding system limits on parameters such as cost, weight and volume.

Technical Management Decision Making - The results of the reliability prediction and optimization analyses were used throughout the development effort on the power conversion and control assemblies. Some specific instances in which engineering and/or management decisions were based on these analyses are:

1. The establishment of part procurement requirements based on accurate application information.

2. The initiation of a circuit and packaging redesign effort for the purpose of minimizing electrical connections.

3. The initiation of extensive engineering and manufacturing investigation which proved welded connections were not needed thus saving the division considerable funds.

4. The selection and functional definition of ground command and automatic with ground command override switching arrangements.

5. The selection of items to undergo stress-strength test to failure investigation.

6. The selection of simplified battery charger designs.

AOSO Summary

As a result of the conversion and control assembly reconfiguration and design improvement program, of which the reliability optimization activities were a portion, the configuration was improved as shown in Table III.

Bibliography

General

1) B. Tiger, M. J. Smith, "Methodology for System Reliability Analysis", Proceedings Eighth National Symposium on Reliability and Quality Control, January 9-11, 1962, pp 135-141.

2) L. R. Webster, "Optimum Redundancy for a Satellite Power System", Proceedings Eleventh National Symposium on Reliability and Quality Control, January 12-14, 1965, pp 568-574.

Redundancy

3) I. Bazovsky, "Reliability Theory and Practice", Prentice-Hall, Inc., Englewood Cliffs, New Jersey 1961, pp 87, 97-126.

4) U. S. Department of Defense, "Reliability Stress and Failure Rate Data for Electronic Equipment"-MIL-HDBK-217", U. S. Government Printing Office, Washington, D.C., 1962, pp 231-248.

5) Department of the Navy Bureau of Ships, "Navy Reliability Design Handbook", U. S. Navy Bureau of Ships, Washington, D. C., 1960, section 1.6, change 10, pp 12-28.

6) H. S. Balaban, "Some Effects of Redundancy on System Reliability", Proceedings Sixth National Symposium on Reliability and Quality Control, January 11-13, 1960, pp 388-402.

7) S. A. Weisberg, J.H.S. Chin, "Reliability and Availability of Some Redundant Systems", Presented at Maintainability Conference at Hanscom Field, Bedford Massachusetts, March, 1963.

Optimization

8) G. Black & F. Proschan, "Optimal Redundancy", Operations Research Journal, September 1959, pp 581-588.

9) B. J. Flehinger, "Reliability Improvement Through Redundancy at Various System Levels", I.B.M. Journal, Vo. 2, No. 2, April 1958, pp 148-158.

10) M. Sasaki, "A Simplified Method of Obtaining Highest System Reliability", Proceedings of Eighth National Symposium of Reliability and Quality Control, January 9-11, 1962, 489-502.

11) R. E. Barlow and L. C. Hunter "Criteria for Determining Optimum Redundancy", I.R.E. Transactions on Reliability and Quality Control, April, 1960, pp. 73-76.

12) M. Sasaki, "An Easy Allotment Method Achieving Maximum System Reliability", Proceedings Ninth National Symposium on Reliability and Quality Control, January 22-24, 1963, pp 109-124.

13) L. R. Webster, "Choosing Optimum System Configurations", Proceedings Tenth National Symposium on Reliability and Quality Control, January 7-9, 1964, pp 345-359.

Systems and Operations Analysis

14) J. A. Connor, "Reliability Predictions for Multi-Mode Electronic Systems", Proceedings Eighth National Symposium on Reliability and Quality Control, January 9-11, 1962, pp. 516-519.

15) Major H. A. Wilkes, "Operational Research - A Prelude to Reliability", Proceedings Eighth National Symposium on Reliability and Quality Control, January 9-11, 1962, pp 516-519.

TABLE I

CONFIGURATION	RELIABILITY MODEL ($r = e^{-\lambda t}$) SHORT = OPEN	SHORT = 0	OPEN = 0	REF.
FUNCTIONAL  $r_1 \neq r_2$ $r_1 = r_2$	$e^{-\frac{\lambda_1 t}{2}} + e^{-\frac{\lambda_2 t}{2}} - 1$ r	$e^{-\lambda_1 t} + e^{-\lambda_2 t} - e^{-(\lambda_1+\lambda_2)t}$ $1-(1-r)^2$	$e^{-(\lambda_1+\lambda_2)t}$ r^2	3,12
SEQUENTIAL  $r_1 \neq r_2$ $r_1 = r_2$	$e^{-\lambda_1 t} + r_{SW}\frac{\lambda_1}{\lambda_2-\lambda_1}(e^{-\lambda_1 t} - e^{-\lambda_2 t})$ $e^{-\lambda t}(1+r_{SW}\lambda t)$			12
VOTER  FLIP-FLOP+AND=r "OR" GATE = R_O	$(3r^2 - 2r^3)R_O$			12
QUAD  $r_1=r_2=r_3=r_4$	$\frac{1}{2}(3r - r^3)$	$r^4 - 4r^3 + 4r^2$	$2r^2 + r^4$	12
IN SERIES WITH ONE SPARE $r_m = r_1$	$r(1+m\lambda t)$			7

TABLE II

Item	Required Reliability	Predicted Reliability	"first cut" Parts Count Prediction
Power Conversion	0.943	0.797	----
Power Control	0.971	0.989	----
Both Assemblies Combined	0.915	0.787	.51

TABLE III

Item	Reliability Requirements	Initial Prediction	Present Prediction	Initial Weight	Present Weight
Conversion Assy.	0.943	0.797	0.995	85	62
Control Assy.	0.971	0.989	0.994	62	32
Combined	0.915	0.787	0.99	147	94

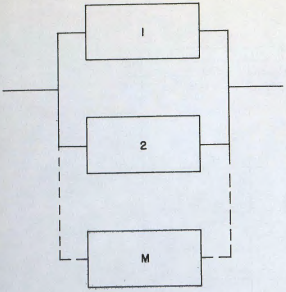


FIGURE 1

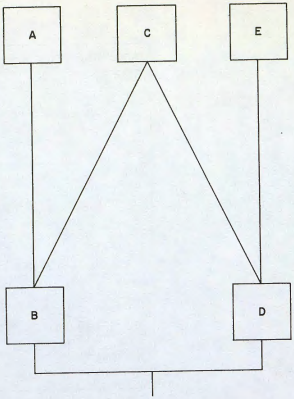


FIGURE 2

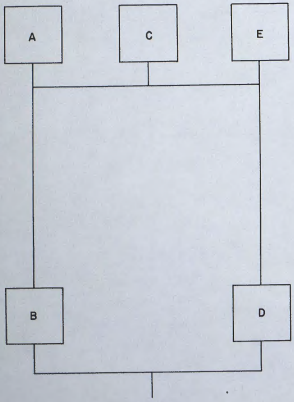


FIGURE 3

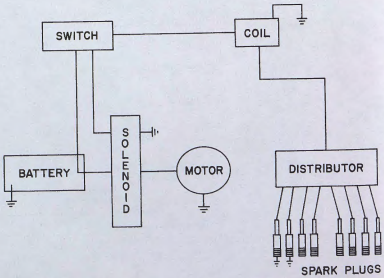


FIGURE 4

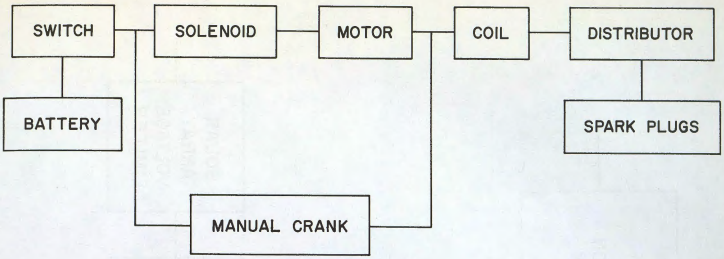


FIGURE 5

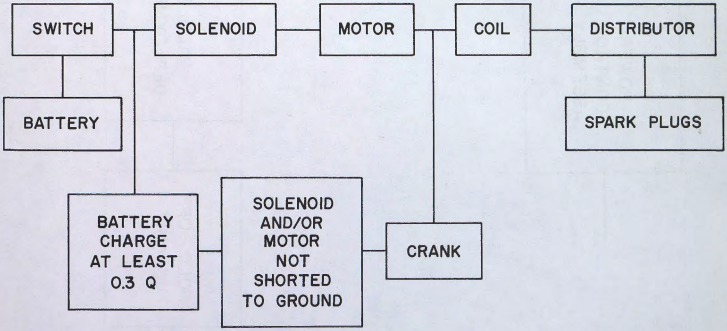


FIGURE 6

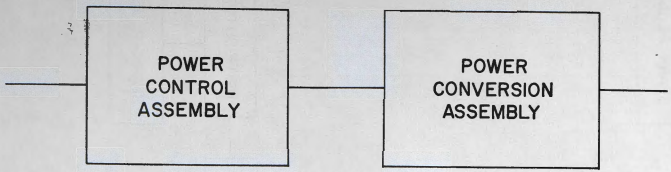


FIGURE 7

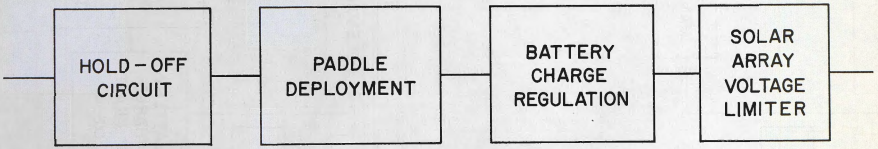
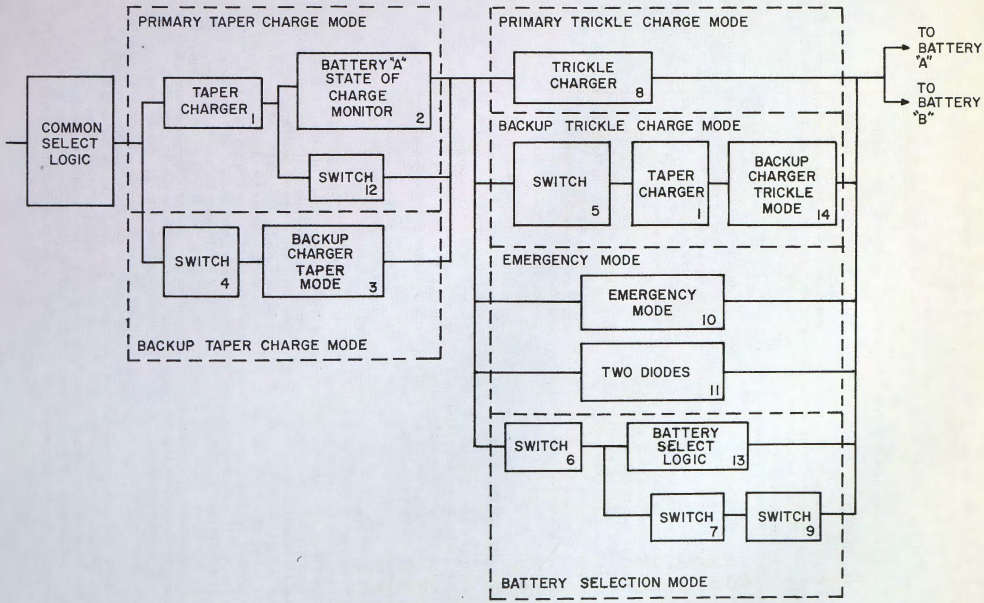


FIGURE 8


PRIMARY TAPER CHARGE MODE
COMMON SELECT LOGIC
TAPER CHARGER 1
BATTERY "A" STATE OF CHARGE MONITOR 2
SWITCH 12
SWITCH 4
BACKUP CHARGER TAPER MODE 3
BACKUP TAPER CHARGE MODE
PRIMARY TRICKLE CHARGE MODE
TRICKLE CHARGER 8
TO BATTERY "A"
TO BATTERY "B"
BACKUP TRICKLE CHARGE MODE
SWITCH 5
TAPER CHARGER 1
BACKUP CHARGER TRICKLE MODE 14
EMERGENCY MODE
EMERGENCY MODE 10
TWO DIODES 11
SWITCH 6
BATTERY SELECT LOGIC 13
SWITCH 7
SWITCH 9
BATTERY SELECTION MODE

323

FIGURE 9